

Check Point Advanced Troubleshooting Workshop (CP-ATWS)

Tämä 3-päivän erikoiskurssi on tarkoitettu Check Point administraattoreille ja tietoturva-asiantuntijoille, jotka haluavat oppia analysoimaan ja ratkomaan Check Point järjestelmien vika-/ongelmatilanteita itsenäisesti. Kurssilla käsitellään mm. FW Monitor, NGX kernel debuggaus, NAT debuggaus, VPN troubleshoot, klusterointi sekä SecureXL ja CoreXL suorituskykyoptimointi.

Ennakkotietosuositukset

Osallistujien tulisi olla käynyt CCSA kurssi tai omata vastaavat tiedot/taidot.

Kurssin tavoitteet

Kurssin käytyään osallistujat osaavat tehdä perusteellisesti ja yksityiskohtaisesti virheanalyysia Check Point ympäristöihin, ja näin ollen parantaa vikatilannepalveluiden vasteaikoja sekä laatua.

Kurssin sisältö

- Yleiset vikatilanne käsitteet
 - o politiikkojen määrittämisen sisäiset prosessit
 - o VPN?1 prosessit
 - o tärkeimmät asetustiedostot
 - o Check Point järjestelmien tilannekuvan määrittäminen
- FW Monitor
 - o mikä on 'fw monitor'?
 - o käytännön esimerkkejä pakettianalysointiin FW MONITORilla
 - o FW MONITOR tulosten analysointi WireShark työkalulla
- Kernel Debug in NGX
 - o Packet flow & Chain Modules
 - o Debuggaus prosessitasolla (fwm, fwd, ...)
 - o Debug Flags
 - o Debugging Tipps
- NAT Debugging
 - o Mikä on NAT?
 - o NAT Debugging periaatteet?
 - o Hide NAT
 - o Dynamic NAT analyysi ja Port Address Translation
- VPN Troubleshooting
 - o IPsec VPN yleisesti
 - o 1.vaihe: IKE SA:n käsittely Main Mode:lla (Aggressive Mode)
 - o 2.vaihe: IPsec SA:n käsittely Quick Mode:lla
 - o VPN kirjautumisen ongelmat
 - "Invalid ID Information"
 - "No Proposal Chosen"
 - "Payload Malformed"
 - o VPN Daemon Debug Mode:lla

- Klusterointi
 - o ClusterXL, Nokia VRRP ja IP Clustering konseptit
 - o ClusterXL:n eri moodit (HA ,Load Sharing)
 - o Klusterointiskenaariot (Hotfix?Installation, Upgrade, ...)
 - o Nokia VRRP ja IP Cluster sisältö
 - o Klusterien ongelma-analysointi
- Suorituskyvyn optimointi SecureXL ja CoreXL työkaluilla
 - o Mikä on SecureXL?
 - o Mikä on CoreXL?
 - o CoreXL (SND, FWD)
 - o SND analyysi Flow Template:lla